A Job Market Signaling Scheme for Incentive and Trust Management in Vehicular Ad Hoc Networks

Nadia Haddadou, Abderrezak Rachedi, Yacine Ghamri-Doudane

A Job Market Signaling Scheme for Incentive and Trust Management in Vehicular Ad Hoc Networks

Nadia Haddadou, Abderrezak Rachedi, and Yacine Ghamri-Doudane

***Abstract*—In collaborative wireless networks with a low infrastructure, the presence of misbehaving nodes can have a negative impact on network performance. In particular, we are interested in dealing with this nasty presence in road safety applications, based on vehicular ad hoc networks (VANETs). In this work, we consider as harmful the presence of malicious nodes, which spread false and forged data; and selfish nodes, which cooperate only for their own benefit. To deal with this, we propose a Distributed Trust Model (DTM^2), adapted from the job market signaling model. DTM^2 is based on allocating *credits* to nodes and securely managing these credits. To motivate selfish nodes to cooperate more, our solution establishes the cost of reception to access data, forcing them to earn credits. Moreover, to detect and exclude malicious nodes, DTM^2 requires the cost of sending, using signaling values inspired form economics and based on the node's behavior, so that the more a node is malicious, the higher its sending cost, thus limiting their participation in the network. Similarly, rewards are given to nodes whose sent messages are considered as truthful, and that paid a sending cost considered as correct. The latter is a guarantee for the receivers about the truthfulness of the message since, in case of message refusal, the source node is not rewarded despite its payment. We validated DTM^2 via a theoretical study using Markov chains; and with a set of simulations, in both urban and highway scenarios. Both theoretical and simulation results show that DTM^2 excludes from the network 100% of malicious nodes, without causing any false positive detection. Moreover, our solution guarantees a good ratio of reception even in the presence of selfish nodes.**

***Index Terms*—Vehicular ad hoc networks, incentive model, malicious nodes, selfish nodes, job market signaling model.**

I. Introduction

In recent years, the emergence of vehicular ad hoc networks (VANETs) has lead them to become a particularly studied field. They consist on smart vehicles, communicating with each other, and, in the case of setting up an infrastructure, with nearby *road side units*. Similar to mobile ad hoc networks (MANETs), VANETs use wireless communications. Nevertheless, their characteristics make them more complex than MANETs. Indeed, the high node velocity range, the extended geographic set up area, and the large size of the network, lead to frequent topology changes, and result in sporadic connections between nodes.

VANET applications can be divided mainly into two categories: infotainment applications and Safety applications [1]. The latter, aims to lower, and ultimately avoid the annual million deaths worldwide caused by road accidents. In this work, we deal with road safety applications, such as road traffic data collection and sharing, accident alert, traffic jam notification. These applications provide information directly related to users' safety, in order to reduce road accidents. Their content is both time and security sensitive. Each content alteration can cause accidents, as in the case where a malicious vehicle disseminates false information.

Integrity, *authentication*, *timeliness*, and *cooperation* are the basic requirements for safety applications. Indeed, each sensed safety event must be sent by an authenticated vehicle, and received in time by all concerned vehicles thanks to the cooperation of vehicles. Moreover, the shared data in safety applications must not be altered without detection in a minimum of time to meet timeliness requirements. These applications can also be critical in case of misappropriation. Indeed, if forged data are shared, this may cause unsafe situations on the road. Therefore, a node should never accept any safety information without guarantee of its truthfulness. Moreover, since safety applications are time sensitive, a node has to make a quick decision about the validity of a received message. This task becomes even more challenging when the communication medium does not rely on any infrastructure, or if that is scattered, making it impossible to validate any information beforehand. In this work, we are interested in these kinds of applications when they are set up in VANETs without the use of any communication infrastructure, thus requiring advanced dissemination algorithms, such as those proposed in [2] and [3].

In a collaborative network such as a VANET, any node dissociation is difficult because of the significant number of nodes comprising the network. On top of that, because of high mobility and the extended set up areas, asymmetric information regarding the behavior of each node is widely disseminated. Therefore, establishing direct connections between nodes becomes challenging, thus encouraging the emergence of malicious and selfish nodes. The purpose of this paper is to bring an effective solution that filters out misbehaving nodes. These nodes can be either *malicious* or *selfish*. Malicious nodes introduce false information or retransmit forged information in a VANET. Selfish nodes serve their own interests and use their resources only for their

N. Haddadou, and A. Rachedi are with Gaspard Monge Computer Science Laboratory (LIGM - UMR 8049), Université Paris-Est, 75420 Champs sur Marne, France. E-mail: {nadia.haddadou,rachedi}@u-pem.fr

Y. Ghamri-Doudane is with L3i Lab, University of La Rochelle, La Rochelle, France. E-mail: yacine.ghamri@univ-lr.fr

own needs. Thus, their cooperation rate is low. However, unlike malicious nodes, these selfish nodes are rational, which means that they can cooperate if it is in their interest.

In order to deal with node scattering, we allocate each node a credit account, which can increase and/or decrease according to its behavior. This credit is useful to obtain advantages within the network, as holding credits allows a node to take part in the network by sending or receiving messages. On the other hand, a node that runs out of credits is evicted from the network. To manage the node credit, we base our solution on an economic model called the job-market model [4], belonging to the signaling models [5]. These models intervene in a case where the different parties may hold asymmetric information [6]. Thus, a model can be used to obtain a general view of node behavior in a VANET. In addition, the high mobility of vehicles and their large deployment area, cause sporadic connections in the network, and infrequent meeting intervals among nodes [7]. Since reputation models need stable connections to obtain actual reputation values, they may take a long time to eradicate one malicious node, only a reputation model for VANET is not enough. The main concept behind signaling models is to exchange signals between nodes. This signal informs about a node's behavior, and then, the truthfulness of the messages it sends. A signal has a cost corresponding to the actual behavior of the node, so that the more a node is malicious, the higher its cost of sending. Thus, this cost is a guarantee of the node's truthfulness. If a sent message is considered as false and thus refused by the neighbors, the emitting node loses its signal cost, which incurs an eviction from the network once its credits are depleted. This paper is an extension of our previous work [8], in which: We propose a novel distributed trust model (DTM^2) for VANETs, inspired from the job market signaling model. In addition, we introduce a prevention mechanism, to detect and evict malicious nodes from the network; and an incentive mechanism that increases the cooperation of selfish nodes.

To summarize, the new contributions of this paper are:

- A Markov chain of DTM^2 is proposed to properly select parameter value, and prove that DTM^2 works well.
- An extensive simulation study is done to show the right behavior of DTM^2, and assess its performance in realistic urban and highway scenarios.

The remaining part of this paper is organized as follows: In Section II we present the related work dealing with trust models in the literature. This is, followed by some definitions and assumptions in Section III and a presentation of economic signaling models to deal with asymmetric information in Section IV. In Section V we present our solution, DTM^2. Then, we model it using Markov chains and present its theoretical results in Section VI. A security analysis is proposed in Section VII and Section VIII presents our performance study including both analytical and simulations results. Finally, Section IX concludes this paper and presents future perspectives.

II. Related Work

There are many solutions proposed in the literature dealing with trust models for mobile ad hoc networks as presented in [9]. These solutions cope either with malicious nodes or selfish ones, but rarely with both of them at the same time. They can be classified into three categories: incentive approaches based on tamper-proof devices, incentive approaches based on infrastructure deployment, and reputation-based approaches.

A. Incentive approaches based on tamper-proof devices

To improve cooperation in a network, existing solutions propose rewards in return of a node's participation, which is the general concept of incentive cost/reward models, as presented in [10], [11]. These solutions use nuggets as method of payment to incite nodes to be more cooperative, and suppose that each node is equipped with a tamper-proof device to manage its nuggets.

In [10] two schemes are proposed to estimate a node's reward for retransmission, the packet purse scheme and the packet trade scheme. The packet purse scheme estimates rewards according to the number of intermediate nodes. However, because of the propagation speed of information in VANETs [12] and the high mobility of vehicles, underestimation and overestimation of the reward may occur frequently, which leads the solution to be ineffective. In the packet trade scheme, the destination node has to reward all intermediate nodes for their forwarding actions, which represents a higher cost if there are many of them. Furthermore, both these schemes deal only with selfish nodes. Then, in [11], the same authors proposed different levels of cooperation for network nodes, according to the number of credits they hold and their desire to cooperate. These levels can make the participation of nodes turn into a quantitative one and not necessarily a constant one, because there is no requirement for a node to keep in constant cooperation, thus leading to a decline in network connectivity.

In [13], an incentive model set up simultaneously with a reputation one ($VIME$) is proposed. Similarly to DTM^2, $VIME$'s incentive model uses both cost and reward values, in addition to signaling values. However, $VIME$'s signaling cost is computed according to the reputation value of the node, so as the more truthful a node is, the less expensive its signaling value will be. But a reputation value in VANETs is versatile, which distorts the model. Likewise, a source node receives a reward for a truthful sent message, its reward is burdened by its neighbors according to their number, and then rewarder messages are sent to the source. Because of the mobility in VANETs, these messages can be lost and the source not completely rewarded, although the credit amount has been subtracted.

B. Incentive approaches based on infrastructure deployment

Incentive is proposed through the game theory as it is the case in [14], where authors enhance the security in mobile ad

hoc networks. They motivate nodes to cooperate by increasing their reputation with an authority, which provides them some privileges in the network. Other proposed solutions in [15], [16], and [17] provide incentive through rewards to intermediate nodes. All these solutions are based on the deployment of infrastructures. In [15], the authors propose FRAME, a fair reimbursement and motivating sweepstake scheme. It copes with the overspending problem that occurs when the number of intermediate nodes grows over time without any limit. FRAME motivates selfish nodes by proposing them a weighted rewarding strategy according to their contribution, computed with their storage time and a number of sprays of others' messages. In addition, to be more attractive, it selects one intermediate node by sweepstakes to be rewarded with a fixed value. However, this solution is limited by the existence of infrastructures, since a source node has to contact an authority to obtain the permission to share its message, and to give beforehand the reward for intermediate nodes to forward its message. Moreover, FRAME does not deal with the presence of malicious nodes. Another incentive solution proposed in [16], encourages selfish nodes to cooperate by proposing rewards to them, with an enhanced security system using Reed-Solomon codes [18] in order to avoid credit fraudulence, by avoiding the cases where a source node can refuse to reward, or where intermediate nodes can ask to be over-rewarded among other cases. Similarly, to enhance security, [17] propose to verify the receipt of all the actions in the network based on a Credit Clearance Service, and then reward the participants. The use of such a method can increase the network delays, and negatively impact its performance.

C. Reputation-based Approaches

Another kind of solution, based on the use of a reputation model for vehicles, is proposed in [19]. The basic idea is to add a criterion to the category of the driver, setting apart, for instance, a law enforcement agent from a regular citizen. To validate a received message, a node asks its neighbors about its validity, and takes it into consideration only if the received responses reach a majority consensus. The limitation of this solution is the generated overhead, and the time that it can take to validate the received data. Another solution uses fairness as a criterion of cooperation by computing reputation values, so that nodes cooperate with each other in a reciprocal way [20]. However, this solution involves huge costs, as it is based on frequent monitoring of the nodes' behavior as demonstrated in [21].

Our solution, DTM^2, is able to cope with the presence of both malicious and selfish nodes in a VANET without any infrastructure. Moreover, it handles the high mobility and asymmetric information of a VANET more easily since the computation of signaling costs and reward values is not based on estimations of their values. DTM^2 creates self-selection among nodes, thus evicting malicious nodes and increasing the cooperation of selfish ones.

III. System Model and Assumption

A. Definitions and assumptions

We consider that our network is composed of malicious, selfish, and good behavior vehicles. The first kind has the worst behavior, which actively attacks the network. Indeed, a malicious vehicle can modify the content of a message before relaying it, either by replacing the information in it with completely new information, or with the opposite information. A malicious vehicle can also send fake messages about false events for its own interest, or treating with its chosen signal value. To avoid being detected, this kind of vehicles can alternate between good and malicious actions.

The second kind is the selfish behavior, which passively decreases the network performance. A vehicle is selfish when it refuses to relay received messages, not to reduce the traffic load, but just to preserve its own resources, such as the channel access time, for its own benefit. Selfish nodes are rational, and do not alter the content of messages.

We assume in the rest of the paper that all the vehicles using DTM^2 to share information communicate via broadcast. To allow such assumption, each participating vehicle is equipped with a trusted platform module (TPM) [22], described in the subsection below.

We assume that a TPM is inviolable, (i.e. a malicious node cannot tamper the recorded credits on its TPM). This assumption, makes impossible to send or receive messages if the node runs out of credit. Furthermore, when a node runs out of credit, we consider that the node is detected and excluded from the network. However, a malicious node can tamper with its signal value. Indeed a vehicle is free to choose its signal value. This value is directly observable by all (because of broadcast transmissions), which allows other vehicles to make decisions about the validity of the shared data with respect to the used signal value.

B. Trusted Platform Module (TPM) functionalities

The TPM is a hardware device proposed by the TPM groupe [22], and used in [23], [24], and [25]. It includes Random Number Generator, SHA-1 Hash Generator, Asymmetric and Symmetric Encryption and Decryption Functions using RSA or Elliptic Curve Cryptography (ECC), which perform cryptography capabilities, while being tamper-proof.

The TPM manages the credit count of nodes. It stores credit in a shielded location, then it computes and deducts the signaling cost, in the case of sent messages; or deducts the price of a received message in case it is validated by the receiver. It also increases credit count when a sent message is accepted by the majority of its recipients. Finally, the TPM stores a fingerprint of the application it is responsible for (e.g. an advanced driver assistance system), which leads it to detecting any changes to the application made by an attacker [24]. Moreover, the TPM meets the real-time requirements by VANETs safety applications according to [26] and [27].

Each embedded TPM in a vehicle has a unique Endorsement Key (EK), generated by the TPM manufacturer, and

securely stored inside it. The public part of this key is visible in the Endorsement Certificate. The EK is only used for the internal workings of TPMs. Moreover, each TPM has an Attestation Identity Key (AIK) and its certification, an alias for the Endorsement key used for identity attestation, generated by the manufacturer, which is generally a 2048 bit RSA key pair with a private and a public key. For anonymity reasons, a TPM can generate multiple AIK pairs, provided that a Trusted Third Party certifies it [23]. We suppose that these pairs of key are loaded by the manufacturer, and do not require any revocation mechanism, even in the case where the vehicle equipped with this TPM is detected as malicious, and forbidden to participate to the system.

To avoid weakening the security of the AIK by signing a lot of data, and so making its cryptanalysis easier, authors in [28] propose to generate a renewable key "signing key" (SK) by the TPM. After signing generated data by an application, a TPM returns to the vehicle a signed version of the messages by its signing key (SK), and attaches a certification of the used signing key for the receivers. This certification consists on a signed version of the SK by the AIK, in addition to the delivered certification by a privacy certification authority (PCA) for the AIK, as presented in [23]. Using this signing process, a receiver is able to authenticate a vehicle with the AIK of its TPM, without holding any key except the public key of PCA.

In addition to the authentication, DTM^2 uses a TPM to ensure confidentiality of the exchanged data. Vehicles should access the shared data only through their TPM, to charge a cost of reception to the receivers. In order to meet this condition, a standard secret key (SyK) is preloaded by the manufacturer in all the TPM to achieve a Symmetric-key encryption for all exchanged messages by applications.

IV. Asymmetric Information in Markets and Signaling Games

Signaling games [5], a type of dynamic Bayesian game with incomplete information, forms the basis of multiple solutions in economics to cope with the lack of information between sellers and buyers about the quality of proposed wares. They refer to a strategic model where two agents interact in a way where one part is informed and the other is not. To inform the other part about hidden information, an agent uses a signal. A signal is an observable characteristic about an individual; it represents a criterion to differentiate between multiple members (the sellers in the example). The high quality productive members in a market choose to use it to inform others about their qualifications. It must have a cost and represents an investment for these users, in order to discourage the others from imitating it.

In the case of a market, a solution to the problem of asymmetric information about the wares, can be the use of different kinds of insurances proposed by the sellers and corresponding indirectly to the sellers' knowledge about the quality of their products. One of the most used signals nowadays is advertising. When a firm is confident about the quality of its products, it pays a significant price to advertise these products. Advertising represents a signal sent to consumers; it represents an investment for the sender but allows him to increase its profits due to the actions consumers take in return. We are interested in reproducing this incentive in trust model in VANETs, because it takes into consideration the lack of information between nodes.

In this section, we adapt one of the well-known examples of the signaling games, the Spence model, also known as job market signaling, to a VANET in order to obtain a functional trust and collaborative network.

A. Job market model

Spence's model or the job market signaling model [29] is generally illustrated by resolving the job market problem, regarding a personnel hiring situation with asymmetric information. An employer has to enroll some candidates and pay them for their productivity but, unlike the candidates, he is not sure of their skills when he hires them. In this case, one part of the market is totally informed (i.e. the candidates) while the other one is not (i.e. the employer). Nevertheless, both of them have to interact with each other.

To attract the employer's attention, a candidate will try to inform him about his productive capabilities by sending him some information as a signal. The chosen signal in this model is education. It is assumed that the level of education does not amount to the skillfulness of a candidate, but it is positively correlated with having greater skills. Therefore, the more a candidate has educational credentials, the more he is considered as competent and productive.

To make it inimitable, the signal has to have a cost that is negatively correlated to productivity. In this case, a degree costs less for an individual with high skills than for one with low skills. An employer proposes to a candidate a wage equivalent to his supposed productivity according to his signal value, so that a candidate chooses the optimum signal (level of education), which maximizes the net return after subtracting the signal cost from the wage.

In order to classify the candidates with respect to their supposed productivity, the employer may create a *Separating Equilibrium*, in which each candidate signals his education level to maximize his benefit. High quality workers obtain a maximum level of education, because it is assumed to be less costly for them, in order to signal it and distance themselves from others. Unlike them, low quality workers study the trade-off between signaling a great value to get a high salary, and signaling a small value which costs them the minimum and obtain the corresponding salary. They often choose the second option.

B. Market vs. VANET

Spence's model distinguishes between workers in the case of asymmetric information by using their productivity. In this paper, we are interested in adapting this concept to distinguish between vehicular ad hoc network users.

Motivated by the similarities between the two, our aim is to perform self-selection in a VANET.

In the case of VANETs, the mobility of the vehicles and the size of the area are so high, that they cause significant dispersion of the nodes and create long and infrequent intervals at which nodes meet. As in a market, there is a spread of asymmetric information, so it becomes difficult to establish valid and truthful links between nodes by, for example, using only a reputation model. For our purpose, we use of a signal which is an observable value by all when sending a message, and whose cost is subtracted from the credit count of the node.

The second similarity concerns motivating candidates by paying them fairly according to their skills, in order to attract the best of employees. In a VANET, this can be translated by using incentive rewards to increase cooperation among nodes. In that way, the more a node participates by sending its own messages or by forwarding others' messages, the more wages it receives. Similarly, the better a node behaves and sends true information, the more its wages increase.

The last point concerns evicting malicious nodes from the network. It is a new goal compared to Spence's model, resulting from our adapting Spence's model to a VANET. For safety applications, we have to ensure that the exchanged messages are not tampered with, and that a source node is not malicious, especially when the application does not depend on any infrastructure. An eviction is the result of the exhaustion of a node's resources (e.g. their credit count). From the start, each node possesses a number of credits, which increases or decreases depending on its behavior.

V. DTM^2: Distributed Trust Model Inspired from Job-Market

Spence's model is adaptable to a VANET, since nodes in this kind of networks also suffer from asymmetric information regarding the behavior of each of them. Because of long and infrequent meeting intervals, it is difficult to establish valid and truthful links between nodes only by using a reputation model. Moreover, Spence's model provides a solution to the common problem found in both VANETs and markets, which consists on how to force their members to reveal their real nature to others. This is obtained by encouraging each member to choose the optimal action for it. Therefore, both nodes and the network are able to benefit, without overloading the network, and without requiring a heavy infrastructure in case of VANETs.

Our solution replaces the academic signal of Spence's model by a value signal, observable by all nodes, and used when sending a message as a guarantee of its truthfulness. The signal cost depends on the remaining credit of each node. Upon their first connection to the network, each node receives the same amount of credit. This credit is used to pay the signaling cost when sending a message, and to decrypt received messages. It increases when a sent message is approved by the majority of recipient nodes.

In the rest of this section, we show how such a model can be instantiated in VANETs for incentive and trust management.

A. Basic working scenario

Fig. 1 illustrates the process of exchanging a message using DTM^2. In this example, node A broadcasts a message, and vehicle B is one of the receivers. First, node A chooses a signaling value Y_A. This value is attached to its message Msg_A, and both of them are sent to its TPM. TPM_A uses the credit count of node A, θ_A, to compute the corresponding cost, C_A, of its signal value Y_A, and then subtracts it from the credit count. To ensure the integrity of the mechanism, the TPM signs and encrypts the message, M_A, which contains both the signal value Y_A and the data to share, Msg_A, using its signing and symmetric keys, and then returns it to node A.

When node A broadcasts message M_A, node B receives it and asks the TPM, TPM_B, to verify the signature and to decrypt the signal value for it in order to evaluate its coherence with the reputation value it holds on node A, $R_B^t(A)$. If the reputation is coherent, then node B accepts the message and asks TPM_B to decrypt the rest of the message, which contains the data. Then, its TPM subtracts the cost of receiving a message, C_{msg}, fixed by the application; and delivers the decrypted data, while returning a signed acceptance message about the received information to node B, which will be sent to the source node. In case B refuses the message, a signed refusal message from TPM_B is sent to source node A.

In both cases of acceptance and refusal, the reputation values of both nodes A and B are updated, for the sent message of A, and for the acceptance or refusal message of B, as described in [30]. Finally, if node A receives a majority of positive returns from its recipients, then TPM_A increases its credit count by a reward, $W_A(Y_A)$, proportional to its used signal value Y_A.

B. Computation of signaling cost

In highly mobile environments, such as the one under consideration, signal Y used by a source node acts as a guarantee about the validity of its messages and its honest behavior. An optimum signal value maximizes the net benefit of a node. This occurs when a signal corresponds to the real behavior of the node, which is unavailable to the network and unknown by its TPM. As the credit count value does not change with mobility, this information can be used as a hint on its behavior, since the better a node cooperates, and the more recipients accept its messages, the more its credit increases thanks to rewards and vice-versa. This information is stored by the node's TPM. The signaling cost, C, is negatively correlated to the credit count, θ, but positively correlated to the signaling value according to the two conditions of the job-market model, as shown in (1).

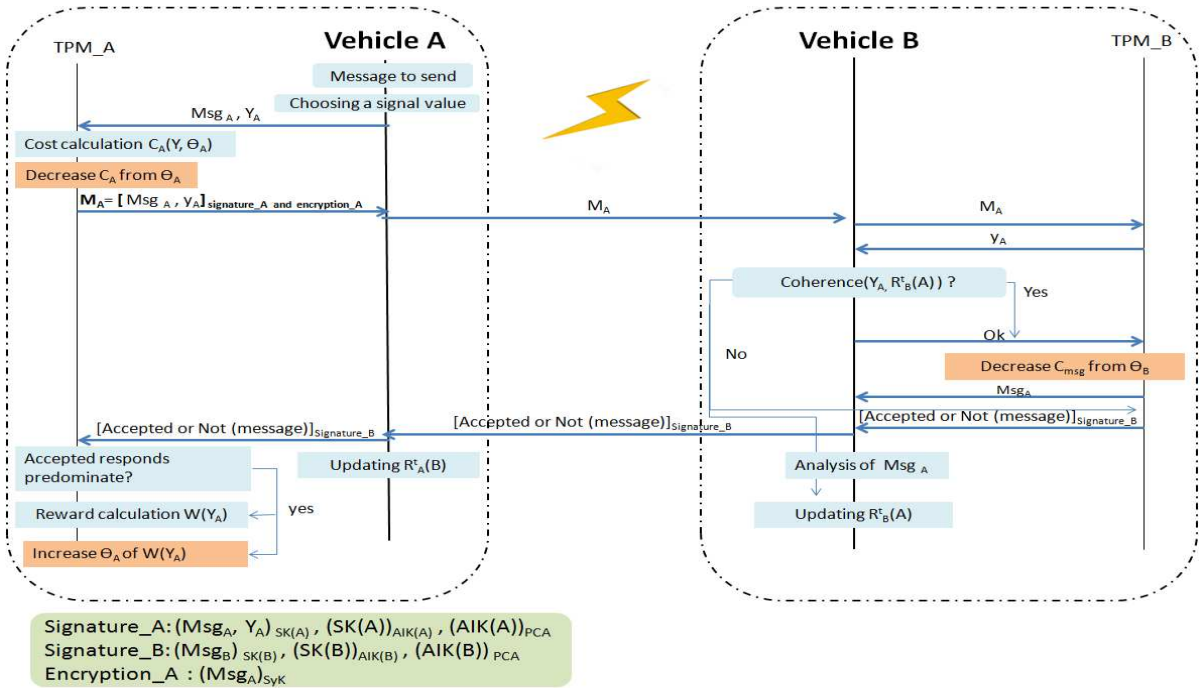


Fig. 1. Process for a message exchange using DTM^2, where vehicle A broadcasts a message and vehicle B is one of the receivers.

$$\begin{cases} C(Y_1,\theta) > C(Y_2,\theta) & For \quad Y_1 > Y_2, \\ C(Y,\theta_1) < C(Y,\theta_2) & For \quad \theta_1 > \theta_2, \end{cases} \tag{1}$$

The signaling cost computation is presented in equation (2). It uses two positive real coefficients β and α. β in order to normalize the signal value regarding the credit count of a node, and α to have a larger impact on the the credit value in the signaling cost computation, such as the higher α, the greater the difference between the signaling costs for the same signal value, paid by different nodes holding different credits. This can be used to detect malicious nodes more or less quickly. The values of β and α are fixed from the start, and are dependent on the type of application.

$$C(Y,\theta) = \frac{\beta \times Y}{\theta^{\alpha}} \tag{2}$$

where β, α, θ >0

To demonstrate the negative and positive correlations required by the model, so that the first condition is met when $\frac{\partial C(Y,\theta)}{\partial Y} > 0$; and the second when $\frac{\partial C(Y,\theta)}{\partial \theta} < 0$ and $\frac{\partial^2 C(Y,\theta)}{\partial Y \partial \theta} < 0$, the derivatives of the cost function with respect to the signal value, the node's credit, and the second derivative, are given in (3).

$$\begin{cases} \frac{\partial C(Y,\theta)}{\partial Y} & = \frac{\beta}{\theta^{\alpha}} > 0 \\ \frac{\partial C(Y,\theta)}{\partial \theta} & = \frac{-\alpha \times \beta \times Y}{\theta^{\alpha+1}} < 0 \\ \frac{\partial^2 C(Y,\theta)}{\partial Y \partial \theta} & = \frac{-\alpha \times \beta}{\theta^{\alpha+1}} < 0 \end{cases} \tag{3}$$

To avoid cheating or security problems when a node pays a signaling cost, the TPM calculates the cost and deducts it from the node's credit. It then encrypts the message containing both the data to share and the signal value by using its secret key, and returns it to the node.

C. Computation of the reward value

To motivate nodes to cooperate, DTM^2 proposes incentive rewards to truthful nodes for their sent messages. A reward value depends on the signal used by the source node, which is the node that detects or forwards a detected event. The secondary goal of this reward is to obtain self-selection of the nodes, which we name a *separating equilibrium*, by inciting them to maximize their benefit by not cheating on their used signal value. The advantage of a self-selection is that it copes with frequent changes to the topology, as often found in VANETs.

In this model, a reward $W(Y)$ is always greater than the cost paid by a node, provided that the node uses a signal corresponding to its credit. The two conditions given in (4), concern the reward on this model. The first condition concerns the rationality of a node. Each node chooses to use a signal Y to maximize its net benefit. This is found when the derivative of the wage is equal to the derivative of the cost with respect to the signal value. The second condition, sets the reference wage value, which needs to be known beforehand by the nodes. Since the credit count of a node hints at the real behavior of a node, the reference wage value depends on it to make it proportional to the real behavior of the node. The reference wage is set by dividing the credit of a node by a coefficient σ, so that the higher the value of σ, the stricter application with regard to the final wage.

$$\begin{cases} \frac{dW(Y)}{dY} & = \frac{\partial C(Y,\theta)}{\partial Y} \\ W(Y) & = \frac{\theta}{\sigma} \end{cases} \tag{4}$$

where σ>0

By replacing $\frac{\partial C(Y,\theta)}{\partial Y}$ with its value, and by isolating θ, we obtain the system in (5).

$$\begin{cases} \frac{dW(Y)}{dY} & = \frac{\beta}{\theta^{\alpha}} \\ \theta & = W(Y) \times \sigma \end{cases} \tag{5}$$

We replace the value of θ by $W(Y) \times \sigma$ for calculating $\frac{dW(Y)}{dY}$ in equation (6), and isolating $W(Y)$ in equation (7).

$$\frac{dW(Y)}{dY} = \frac{\beta}{(W(Y) \times \sigma)^{\alpha}} \tag{6}$$

$$W(Y)^{\alpha} \times \frac{dW(Y)}{dY} = \frac{\beta}{\sigma^{\alpha}} \tag{7}$$

The resolution of equation (7) is obtained by an integration by parts with respect to Y, over an interval $0 \leq Y \leq \infty$ as is described in equation (8) and solved in equation (9).

$$\int W(Y)^{\alpha} \times \frac{dW(Y)}{dY}\ dY = \int \frac{\beta}{\sigma^{\alpha}}\ dY \tag{8}$$

$$\frac{[W(Y)^{\alpha+1}]}{\alpha+1} = \frac{\beta}{\sigma^{\alpha}} \times [Y] \tag{9}$$

This gives us the final equation of the wage shown in (10):

$$W(Y) = \left(\frac{\beta \times (\alpha+1) \times Y}{\sigma^{\alpha}}\right)^{\frac{1}{\alpha+1}} \tag{10}$$

The reward value is added to the credit count of a source node by its TPM, providing that its sent message is validated by the majority of recipients. To verify this, each recipient notifies its own TPM about its decision regarding a received message, and an encrypted message about its decision of acceptance or not is sent to the source node. If the number of accepted message notifications is higher than the number of refused message notifications then the majority is reached. The acceptance or refusal message notifications are encrypted to ensure their integrity, and to avoid the case where a node accepts the received information but sends a refusal message to sabotage the source.

D. Optimal signal value

This model is designed in such a way that a node makes the maximum benefit when it uses the optimum signal value $Y^{\star}(\theta)$ with regard to its credit, θ. DTM^2 incites vehicles to chose their optimal signal value because a signal value is directly observable by all, and mainly because it is directly related to the remaining credits of a vehicle due to its inducing cost. So revealing the optimal signal value, reveals the remaining credits, and then the real behavior of a vehicle.

The optimum signal for each node is obtained from equation (10), by replacing $W(Y)$ with $\frac{\theta}{\sigma}$. The result is given in equation (11).

$$Y^{\star} = \frac{\theta^{\alpha+1}}{\sigma \times \beta \times (\alpha+1)} \tag{11}$$

Failure to respect $Y^{\star}$ causes a shortfall or a loss in credit, as illustrated in Fig. 2. This figure depicts two curves representing the signaling cost of two nodes, and another curve showing the received wage when the sent message is accepted. The first source node possesses 150 credits (i.e it has behaved well), and the second source node possesses only 40 (i.e it has behaved badly), given that the initial credit of the application $\theta_{initial}$ is 100 credits. These curves show results for different signaling values ranging from 0 to 100, and are obtained by setting $\beta = 3.5 \cdot 10^4$, α=2.3, and σ=5. We notice that the wage of the first node is more advantageous. But a shortfall is present for both when they do not use the optimal signal values, which are $Y_1^{\star}$ and $Y_2^{\star}$, respectively.

The net benefit NB of the two nodes is observable in Fig. 2. It is at its maximum when the signaling value equals $Y^{\star}$. Its equation is given in (12) and the results using the same parameter values as before are illustrated in Fig. 3.

$$\begin{aligned} NB &= W(Y) - C(Y,\theta) \\ NB &= [\tfrac{\beta \times (\alpha+1) \times Y}{\sigma^{\alpha}}]^{\frac{1}{\alpha+1}} - \tfrac{\beta \times Y}{\theta^{\alpha}} \end{aligned} \tag{12}$$

Fig. 3 presents the curves of the net benefit for the two source nodes. We notice that the curve of the second node, which is less truthful than the first, decreases faster when it does not respect its optimum signal $Y^{\star}$. This clearly shows that because of bad behavior, nodes quickly exhaust their credit and are therefore evicted from the network.

E. Received message acceptance process

The second way to encourage nodes to cooperate is to create the need for holding credits and earning them. For this reason, decrypting the received message is paid in this model. In the case where a node is selfish, its credit decreases slowly because of its non existent or insufficient cooperation. To secure this part of the model, the cost of a received message, C_{msg}, is fixed by the application, and equals the cost of sending a message for a node holding $\theta_{initial}$ credits divided by a positive real coefficient μ, so $C_{msg} = C(Y^{\star}, \theta_{initial})/\mu$, so that the higher the value of μ, the less a node pays for a received message. This cost is subtracted from a receiver node's count by its TPM. This is only done in a case of acceptance by the recipient. The validation decision is made with respect to the following two criteria:

- The reputation of the source node, held by the receiver.
- The used signal value advertised by the source node.

The used reputation, $R_r^t(s)$, belongs to [0, 1], and is calculated at time t by the Receiver node r with respect to the source node, s. This reputation is local, based on directly observed behavior, and is not shared in the network. If it is too bad, i.e. $R_{r(s)}^t$ is less than a certain threshold ρ, it becomes an elimination criterion for the received message. This criterion is very important at the start of the application, when all the nodes have the same number of credits, thus they use the same signaling value. Its calculation

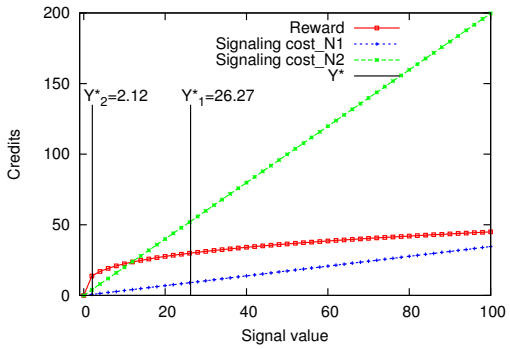


Fig. 2. Cost and reward curves for different signal values, for both N1 and N2, first and second source nodes.

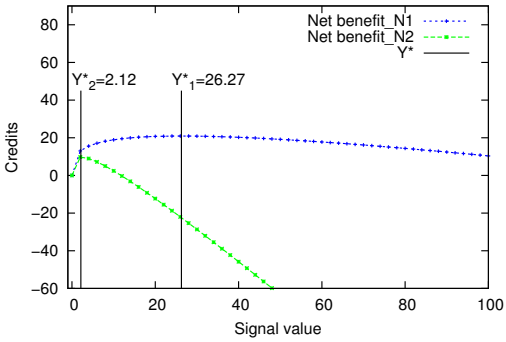


Fig. 3. Net benefit curves for different signal values, for both N1 and N2, first and second source nodes.

is done in equation (13), where $\psi_r(s)$ is the value of the last observation made by node r concerning node s, and ω represents a fading factor to give a higher or a lower relevance value to past observation values. Both of them belong to range $[0, 1]$.

$$R_r^t(s) = \omega \times R_r^{t-1}(s) + (1 - \omega) \times \psi_r(s) \qquad (13)$$

After verifying the reputation criterion, a recipient node can base its acceptance on the signal used by the source. The minimum accepted signal is fixed to $Y^\star(\gamma \cdot \theta_{initial})$, which represents the optimal signal value for a node detaining only $\gamma \cdot \theta_{initial}$ of credits.

F. Credit Safeguard Technique

To avoid good behavior nodes running out of credit and being wrongly detected as malicious due to VANET's characteristics, we introduce an additional rule in DTM^2 operation. Indeed, since VANET nodes are very mobile, frequent changes to the network topology may have a negative impact on the premise on which DTM^2 is based, namely paying for received data and being rewarded for sent data. In some cases, when a node does not detect enough events, or is not elected[a] to retransmit enough messages despite its good behavior, there could be an imbalance between the number of messages sent, which will be low, compared to the number of accepted ones. Therefore, a node could spend all its credit paying to access received messages without earning enough credit through its own sent messages, and could therefore be excluded from the network. Note that, unlike a theoretical model, where the probabilities of receiving or sending messages are equal for all nodes, this problem may occur in some real life situations.

To tackle this, we assumed that if a node's credit level is too low ($\theta \leq \theta_{initial} \times \eta$), where η is a positive real value in the range $]0, 1[$[b], it does not accept received messages (i.e does not pay to decrypt a message and so access its content), until it earns enough credits to exceed the threshold recommended by the application of $\theta \leq \theta_{initial} \times \eta$. This can occur after more cooperation in case of a selfish node, and after changing the road direction or simply after some time for good behavior node. The value of η depends on the nodes' distribution in the network, in order to fade inequality related to the credit earning opportunities of a node, such as sending detected events or forwarding others' messages.

[a]in order to avoid the well known "broadcast storm" [31] problem, data dissemination protocol such as ADCD [2], on which DTM^2 is built upon, make use of election processes to chose the forwarders.

[b]]0,1[notation is equivalent to the open interval (0,1) in the paper.

VI. DTM^2 Parameter Optimization and Adaptation Study

To adjust DTM^2's initial parameters and study its performance, we propose a Markov chain-based model. In our model, we take into consideration the network characteristics, such as message collision probability, the vehicle's transmission range, the event frequency, and the connectivity between the nodes, to model a sufficiently realistic network with DTM^2 set up on it. From this model, we are able to obtain malicious node detection probabilities with its corresponding timing. Moreover, our model provides the detection probabilities of well-behaved and selfish nodes, while the former corresponds to the probability of false positive exclusions in the network.

Indeed, we propose using a Markov chain to model the credit change for a node in the network, according to its behavior. A state in our model represents a node's credit count value, θ. This value belongs to a range $[0, \theta_{max}]$, so that $(\theta_{max} + 1)$ is the number of states in our Markov chain. The transition probabilities of our model represent all the actions that can modify a node's credit (i.e. increase, decrease or stagnation), such as sending a message and paying a cost, or being rewarded for it.

We model road event detection as a Poisson process $P(x = k)$, with λ as arrival intensity. The initial state in our model is represented by the initial credit that a node receives the first time it joins the application. The final state is reached when the credit runs out and is equal to zero, and therefore the node is excluded from the application. The Markov chain for DTM^2 is illustrated in Fig. 4, and the marking system used throughout the theoretical study are listed in Table I.

One of the aims of this model is to reach stationary probabilities, and to find the upper bound false positive

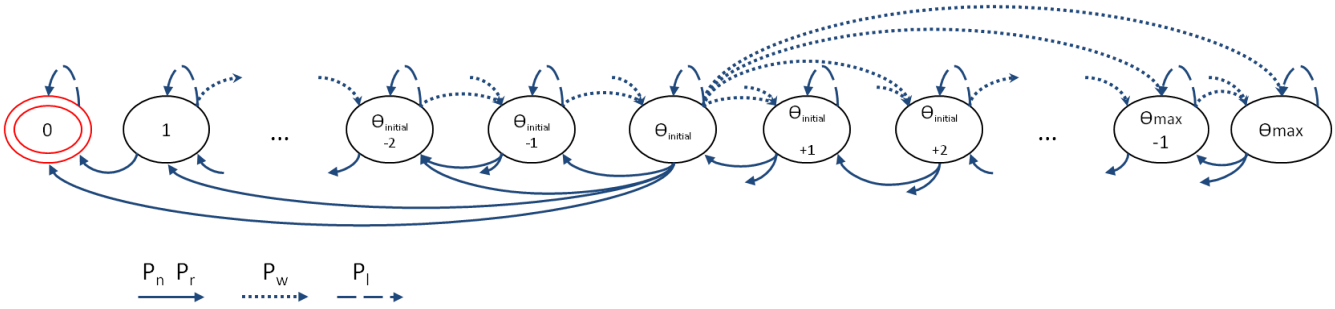


Fig. 4. Markov chain for DTM^2

TABLE I
NOTATIONS

P_t	probability of having a received message to forward
P_c	probability of collision
θ_i	credit value at state i
P_m	malicious behavior probability
P_g	good behavior probability
P_s	selfish behavior probability
λ	arrival intensity in Poisson process for detected events
$P[\theta_i][\theta_j]$	transition probability from θ_i to θ_j
P_f	probability for a source node's message to be refused by its neighbors
P_v	probability for a source node(s message to be validated by its neighbors
Pdf_B	probability density function of a binomial distribution
π	stationary probability for a vehicle to be connected with the others
$P(x=k)$	probability of having k events to detect according to Poisson process
P_n	probability of credit decrease because of no received reward
P_r	probability of receiving a message
P_w	probability of updating credit with a Reward
P_l	probability of credit stagnation

detection probability of DTM^2. To this end, we study the detection probability for each node, by assigning it a behavior percentage for each kind of behavior (malicious, selfish, and good), so that their sum is equal to one. In the following part, we discuss all the possible state changes of our model.

A. Credit Decrease Related to Message Collisions, or Message Refusals

According to our model, a node's credit can decrease in three cases: message collision, neighbor's refusal to accept the sent data, and when paying the cost of decrypting a received message.

When a node detects an event, or retransmits a received message, it pays a cost corresponding to sending a message. However, in some cases, messages are lost because of collisions related to VANET network characteristics, as described in [32]. Therefore, in this case, the source node will receive no rewards. Moreover, in the case when the neighbors of a source node consider its sent message as false, they refuse to accept it with probability P_f, and the node will not receive a reward for it. This probability is referred to as credit decrease because of no received reward (P_n) probability. The probability of holding θ_j credits after having θ_i in the beginning is computed as described in equation (14), so that θ_j is the node's credit after subtracting a cost $C(Y^\star(\theta_i),\theta_i)$ according to the cost equation presented in (2), and the optimum signal value $Y^\star$ for a credit θ_i shown in equation (11).

$$P_n[\theta_i][\theta_j] = \left(\frac{1-P(x=0)}{N} + P_t\right)\Upsilon(P_c+(1-P_c)\times P_f), \tag{14}$$

where θ_j= θ_i-$C(Y^\star(\theta_i),\theta_i)$, and $\theta_j \geq 0$

P_c parameter used in equation (14) represents the probability of a message collision according to the nodes' density in VANETs, as described in [32].

There are two cases where a node sends a message. The first one is when the node itself detects an event, represented by the probability $\frac{1}{N}$, such as N is the number of nodes in the network. This probability depends on the Poisson process, with at least one event occurring with probability $1-P(x=0)$. The second case is when a node receives a message and forwards it with the probability P_t, so that retransmission from one node occurs only once per message (cf. section (VI-B)).

Next, our model computes the P_n probability according to the node's behavior probability (good, P_g, selfish, P_s, or malicious, P_m). If the node is good, the probability of sending a message with the right signal is equal to 1. For a selfish node, its probability of sending depends on its credit count, so that it will not cooperate if it has enough credit. The

third behavior is malicious, where nodes always choose their own sending signal and thus the cost that is most suitable for them. For example, a malicious node sets a threshold as the initial credit value, $\theta_{initial}$, so that if its credit count, θ_i, is higher than this threshold, it chooses to use the optimum signal value corresponding to its credits, $Y^\star(\theta_i)$. Otherwise, it uses the optimum signal value for a threshold credit value, $Y^\star(\theta_{initial})$, provided that it can pay the corresponding cost. A malicious node chooses to "cheat" like this in order to avoid having a small signal value for its sent message, which can be why its neighbors might refuse to accept its message. Υ, represents the sum of a node's behavior probabilities of sending messages according to the threshold $\theta_{initial}$, it is computed as shown in equation (15).

$$\Upsilon = \begin{cases} P_g + P_s & If\ \theta_i \leq \theta_{initial}, \\ P_g + P_m & Otherwise, \end{cases} \tag{15}$$

where $P_g = 1 - (P_s + P_m)$

Secondly, the probability that the neighbors refuse the sent data, P_f, is computed according to a threshold for the used signaling value, Y. During our calculations, we set the threshold to $Y^\star(\theta_{initial} \times 0.2)$, as we consider that this value represents a suitable minimum acceptable signal to consider received data. This probability is presented in equation (16). Its second line replaces the reputation parameter used in the DTM^2 model to validate received information or not. So, here we use the behavior value instead of the real-time reputation value, as we do not have the latter in the theoretical model.

$$P_f = \begin{cases} 1 & If\ Y < Y^\star(\theta_{initial} \times 0.2), \\ P_m & Otherwise, \end{cases} \tag{16}$$

In the case where the source node has predominantly malicious behavior, P_m, and its credit is below the fixed threshold, $\theta_{initial}$ in our model assumption, the probability of sending a message that will be refused changes because of the used signal, Y, which is "false". In this case, instead of using $Y^\star(\theta_i)$, the node uses $Y^\star(\theta_{initial})$ as signal value. The corresponding probability to change from θ_i credits state to θ_j credits state because of a collision, or a refusal of reward is presented in equation (17) in the case where $(\theta_i < \theta_{initial})$.

$$P_n[\theta_i][\theta_j] = (\frac{1 - P(x=0)}{N} + P_t)P_m(P_c + (1 - P_c) \times P_f) \tag{17}$$

where

$$\theta_j = \theta_i - C(Y^\star(\theta_{initial}), \theta_i), with\ \theta_j \geq 0$$
$$P_f = P_m$$

B. Credit Decreases by Paying a Cost for Message Reception

To access a received message considered as valid, whether it uses good signaling value for the message, or it holds a good reputation value on the source node, a node has to pay a reception cost. This cost, C_{msg}, is fixed by the VANET application to $C(Y^\star(\theta_{initial}), \theta_{initial})/\mu$, so that the larger μ is, the lower the message reception cost for a node. This allows a node to accept more messages, but it can also lower the cooperation of selfish nodes since they will need fewer credits. The probability of moving from θ_i detaining credit state to θ_j is computed in equation (18) with the probability of reception, P_r. It depends on the probability that some nodes detect an event and that a node receives their messages by being their neighbor at that moment.

$$P_r[\theta_i][\theta_j] = (1 - P(x=0))\Phi(1 - P_c), \tag{18}$$

where

$$\theta_j = \theta_i - C_{msg}, and\ \theta_j \geq 0$$
$$\Phi = \sum_{m=1}^{N-1} Pdf_B(m, \pi, N-1)\frac{m}{N-1}$$
$$Pdf_B(m, \pi, N-1) = \frac{(N-1)!\ \pi^m (1-\pi)^{N-1-m}}{(m!\ (N-1-m)!}$$

Here, Φ represents the probability that m nodes among all the nodes in the network except source one, i.e. $(N-1)$ nodes in total, receive at least one message, corresponding to one detected event, from one source node, with π representing the stationary probability for a node to being connected with the others, so as its average connectivity degree is $(N-1)\pi$. P_r is based on the probability density function of a binomial distribution, $Pdf_B(m, \pi, N-1)$, presented in [33], which computes the probability for m nodes, among $(N-1)$, to receive the sent message, with a probability π. Then, $\frac{m}{N-1}$ represents the probability that the concerned node belongs to those that have received the message. To obtain all the possibilities for receiver nodes' number, a sum is computed from m=1 to $N-1$. Finally, this probability takes into consideration the collision factor to account for lost messages caused by collisions.

We suppose in DTM^2 that the probability of having a message to forward, P_t, has the same value that the probability of reception of a message, with the assumption that each node retransmits a received message once. This probability is described in equation (19).

$$P_t = (1 - P(x=0))\ \Phi\ (1 - P_c) \tag{19}$$

C. Credit Updating because of a Reward

The DTM^2 model is based on inciting nodes to cooperate and behave well. The reward, $W(Y)$, has to be attractive, but some conditions have to be met before a node is rewarded, like a node's neighbors validating the sent data. A sent message is considered as truthful in the eyes of another node if its reputation on the source node is not too bad, i.e. $P_m > \rho$, and if the used signaling value is not too small. In DTM^2, the signal threshold for accepting a message is fixed to $Y^\star(\gamma \cdot \theta_{initial})$ during our implementation. If the conditions are met, the reward is computed according to the signal value, Y, used by the source. The probability of a node updating its credit with a Reward, P_w, is computed below, in equation (20).

$$P_w[\theta_i][\theta_j] = \left(\frac{1 - P(x=0)}{N} + P_t\right) \Upsilon\ P_v, \tag{20}$$

where

$$\theta_j = \theta_i - C(Y^\star(\theta_i), \theta_i) + W(Y^\star(\theta_i)), \quad 0 \leq \theta_j \leq \theta_{max}$$

$$\Upsilon = \begin{cases} P_g + P_s & If\ \theta_i \leq \theta_{initial} \\ P_g + P_m & Otherwise \end{cases}$$

$$P_v = \begin{cases} 0 & If\ (Y <= Y^\star(\gamma \cdot \theta_{initial}))\ Or\ (P_m > \rho) \\ 1 - P_m - P_c & Otherwise \end{cases}$$

so that $P_v \geq 0$

In the case of sending a message, the probability of receiving a reward depends on that of detecting or retransmitting an event, added to that of paying a cost. Consequently, as in earlier cases, the probability differs according to the node's behavior. If the node has sufficient credit, greater than the initial credit, then both good and malicious nodes participate, and use the correct signal value corresponding to their credit, $Y^\star(\theta_{initial})$. Otherwise, when a vehicle is running out of credits (i.e. the remaining credits are below a defined threshold), the vehicle becomes more interested in cooperating, even if its main behavior is selfish. They will do so in a different way, so that good and selfish behaviors pay the corresponding signal cost, $Y^\star(\theta_i)$, and receive a reward, $W(Y^\star(\theta_i))$, according to the probability in equation (20). A malicious node with a low credit level, chooses to "cheat" and uses a suitable signaling value for it, $Y^\star(\theta_{initial})$. Its probability differs in the θ_j value, because of the paid cost, $C(Y^\star(\theta_{initial}), \theta_i)$. The used signal is that of a node holding $\theta_{initial}$ value, but the cost is according to its actual credit, θ_i. The received reward in this case is $W(Y^\star(\theta_{initial}))$. Its rewarding probability is described in equation (20), with the same definition for P_v as in earlier.

D. Credit Stagnation

The final case is when a node does not send or receive a message, so its credit value does not change. The probability of credit stagnation, P_l is described in equation (21).

$$P_l[\theta_i][\theta_i] = 1 - \sum_{\theta_j=0}^{\theta_{max}} P[\theta_i][\theta_j] \tag{21}$$

Finally, we describe the final state of our model, when the node's credit runs out, so it cannot participate in the network any longer, with the equations in (22).

$$\begin{aligned} &P[0][0] = 1 \\ &P[0][\theta_j] = 0 \quad For\ \theta_j > 0 \end{aligned} \tag{22}$$

E. Adjusting DTM^2's parameters

To improve DTM^2 results and adjust its performance according to the requirements of VANETs safety application, we study the impact of the different parameters involved. First, we study the initial credit value, $\theta_{initial}$, combined to α, the credit's power factor, since they affect the signal computation. Then the variations of the coefficient of the reference wage value, σ, which directly impacts the reward value computation. Finally, we study the coefficient of the reception cost value, μ. The variation of these parameters has an impact on how much and how fast a node can spend or earn credits on the network. This directly influences malicious node detection and false positive percentage.

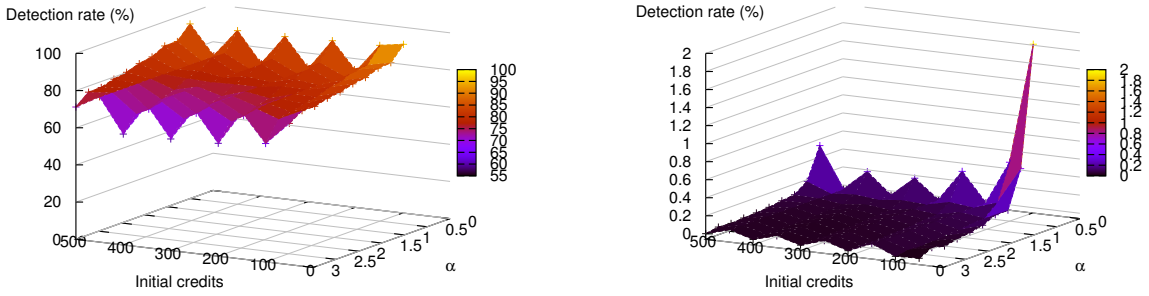
1) Impact of $\theta_{initial}$ Combined to α: Our solution, is based on secure credit management. It begins with the initial credit value assigned to the nodes. A large initial value allows greater participation and interaction between nodes, thus deepening their knowledge of the network members. However, the frequent topology changes and the high mobility of VANETs, enable malicious nodes to extend their lifetime before their exclusion thanks to their high level of credit, as well as increasing the damaging effects they have on the network.

We study the performance of DTM^2 according to the variations of both $\theta_{initial}$ and α because of their simultaneous use in equation (2). An expensive signaling cost, due to a small value of $\theta^\alpha_{initial}$, shortens the exclusion delay for malicious nodes by quickly exhausting their credits. However, it also dangerously increases the false positive percentage by limiting the margin of error for good nodes. Fig. 5 illustrates the percentage of malicious node detection, with $\theta_{initial}$ set to each one of these values: 50, 100, 200, 300, 400, and 500, and with α set to $0.5, 1, 1.5, 2, 2.3, 2.5$, and 3. The detection percentage of malicious nodes with $\lambda = 1$ at 1000s is presented in Fig. 5(a).

We noticed a small peak when the pair $(\theta_{initial}, \alpha)$ is minimal and equals to $(50, 0.5)$. For other combinations, the detection rate decreases faster with variations of α's than with those of $\theta_{initial}$. This is due to the exponential link between the signaling cost and α. By varying only one parameter in the pair, according to the same factor, say 6, we obtain different percentages, so that the detection with $(300, 0.5)$ equals 93%, and that with $(50, 3)$ equals 75%.

Fig. 5(b) illustrates false positive percentage, which represents the percentage of erroneous detections. As before, we modify both $\theta_{initial}$ and α, and obtain a high peak for the pair $(50, 0.5)$, so that the false positive percentage is around 1.9% at 1000s, while it equals to 0.0074% for the pair $(100, 2.3)$. We notice then that, the lower the value of $\theta^\alpha_{initial}$, the greater the percentage of false positives. In the rest of this study, we choose intermediate values for the pair $(\theta_{initial}, \alpha)$, to obtain large percentages of malicious node detection and minimal false positive. Therefor, the couple $(100, 2.3)$ seems to be the best trade-off and is used in the rest of this study.

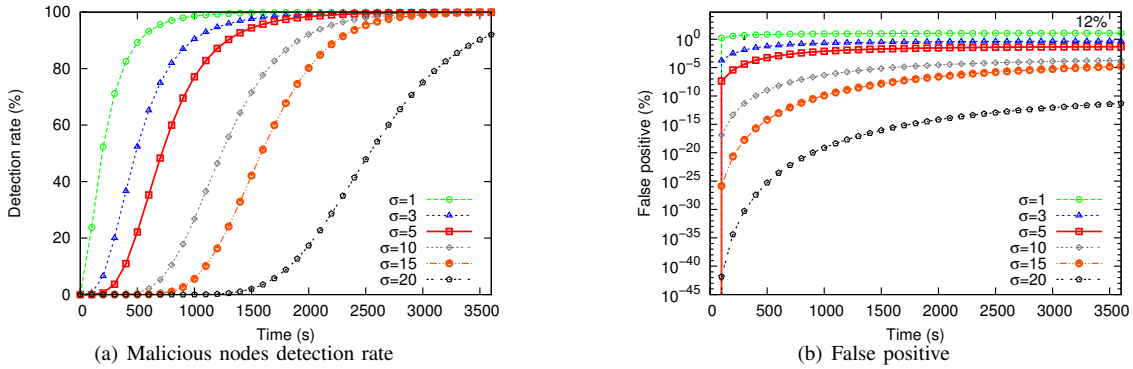
2) Impact of σ: After studying the different signaling cost values and their impact, we are interested in the different values of the reward. According to the system presented in (4), σ increases or decreases the reward value reference, so that it is equal to $\frac{\theta}{\sigma}$. Fig. 6 shows the performance of DTM^2 according to the variation of σ in the set $1, 3, 5, 10, 15$, and 20, with $\lambda = 1$.



(a) Malicious node detection rate

(b) False positive

Fig. 5. Malicious node detection and false positive percentage according to multiple value of signaling cost according to both $\theta_{initial}$ and α, with $\lambda = 1$.



(a) Malicious nodes detection rate

(b) False positive

Fig. 6. Malicious nodes detection and false positive percentage according to multiple value of reward according to σ, with $\lambda = 1$.

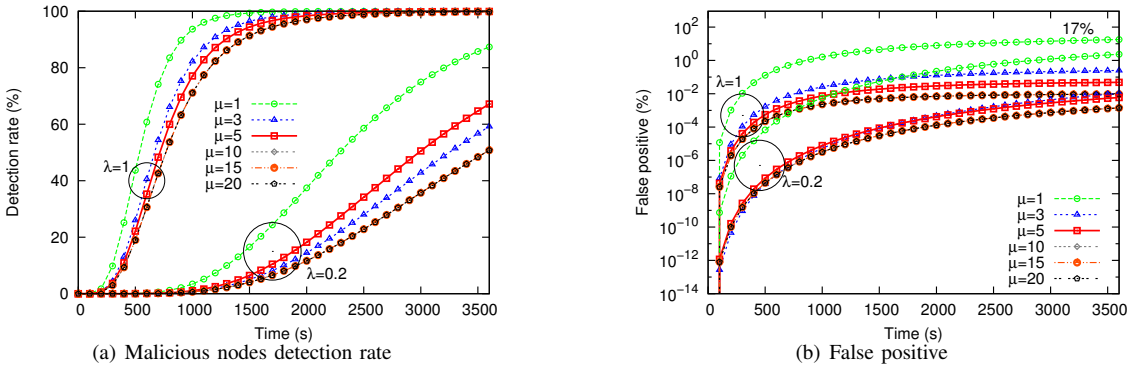
Fig. 6(a) illustrates the malicious node detection percentage. We noticed that the first detection occur at 100s and 1500s, for $\sigma = 1$ and 20, respectively. So, there is a positive correlation between the value of σ and the value of the detection delay. Therefore, as σ increases (i.e. the reference reward value increases) the detection time increases as well. We conclude that handing out large rewards to nodes, as in the cases where $\sigma = 15$ or 20, creates credit overflows, thus debilitating the main premise of DTM^2, which consists in depleting credits for malicious or non cooperative nodes.

As we observed before, the optimal parameters for a high detection percentage, also cause higher false positive results. Fig. 6(b) depicts the false positive percentages. The false positive percentages are very low, except for $\sigma = 1$, which is the case where the rewards are low and that yields the quickest malicious node detection and eviction. Therefore, handing out small rewards can deplete the credits of good behavior nodes, and exclude 12% of them. For the rest of this study, we choose 5 as the value of σ. According to our results, this value represents the best trade-off between malicious node eviction and false positive decrease.

3) Impact of μ: The last parameter to study is μ. This parameter is responsible for the variations of the reception cost. Optimizing this value is important, as it has an impact on both the detection of malicious node, and the cooperation of selfish nodes. Since this value controls the reception cost of a message, malicious and selfish nodes should pay to decrypt messages to remain informed of the road traffic, which can deplete the credits for the malicious and exclude them later if they receive no rewards. Moreover, it encourages selfish nodes to cooperate, by increasing their need to earn credits.

Fig. 7(a) depicts percentages of the malicious node detection for $\lambda = 1$ and 0.2. With $\mu = 1$, the cost of sending and receiving a message are equal for a node holding $\theta_{initial}$ credits. Therefore, for this value of μ, the reception cost is high since a node receives much more messages than it sends.

We notice a faster detection rate for small values of μ, so that at 1000s, the percentage is equals to 93% for $\mu = 1$, 77% for $\mu = 5$, and 71% for $\mu = 20$ when $\lambda = 1$. Hence, the highest is μ, the lowest is the percentage. When $\lambda = 0.2$, the percentages are 74%, 42%, and 35%, for $\mu = 1$, 5, and 20, respectively, at 3000s. However, the false positive percentage for $\mu = 1$ in Fig. 7(b) is worse than for other values, so that it is equal to 17% with $\lambda = 1$ at 3600s, and to 2% with $\lambda = 0.2$, compared to 0.048% and 0.000059%, respectively, when $\mu = 5$. As before, we choose a trade-off between malicious node detection and false positives. This is achieved when $\mu = 5$, which will be used in the rest of



(a) Malicious nodes detection rate (b) False positive

Fig. 7. Malicious node detection and false positive percentage according to multiple value of reception cost according to μ.

our study.

VII. Security Analysis

Changing behaviors is one of the most important points to deal with for a Trust model. DTM^2 avoids this by forcing vehicles to pay for each message to send, so that choosing a higher signal value adds an implicit guarantee to the sent data. However, the cost of a chosen signal value is more expensive when the remaining credits are low.

A vehicle using DTM^2 bases its confidence on received information on two criteria. The first one concerns the reputation held on the source vehicle. Reputation values are not shared between members, to avoid overloading the network. So a vehicle detains a reputation value about another one only in the case where they were neighbors. The second criterion concerns the signal value chosen by the source vehicle: it must be higher or equal to the minimal accepted signal value fixed by the application.

In the case where vehicles refuse to validate some received data (because they sense the opposite of this information), the source vehicle will not be rewarded, and therefore it will not recover its paid sending cost. The cost of sending is higher for a vehicle detaining few credits, in order to restrict their participation in the network, and to motivate vehicles to always keeping an average level of credit by behaving well. A changing behavior vehicle will see its credits decrease very quickly when its behavior is malicious, and they will never or very slowly increase if it changes behavior. This, in addition to the decrease of its reputation value held by its direct neighbors.

Fig. 8 illustrates the detection percentage when nodes alternate between good and malicious behaviors. These results are obtained through mathematical analysis using our Markov chain model. We clearly notice that all nodes behaving maliciously at least 50% of the time are detected over time. In Fig. 9, we change the value of the parameters α to 1 instead of 2.3, and σ to 1 instead of 5. This allows to obtain a faster malicious nodes detection that affects even the vehicles that are malicious less than 50% of the time.

The choice of the parameters depends on the definition of a malicious vehicle. The parameters of our solution allow

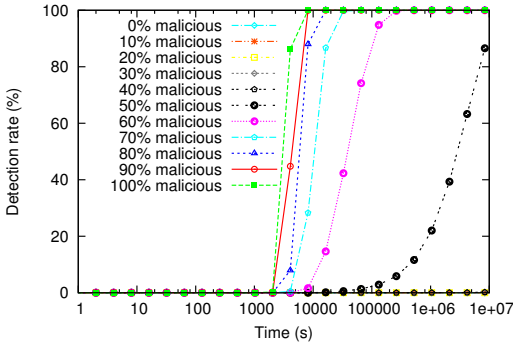


Fig. 8. Nodes detection percentage according to multiple malicious behavior with α=2.3 and σ=5

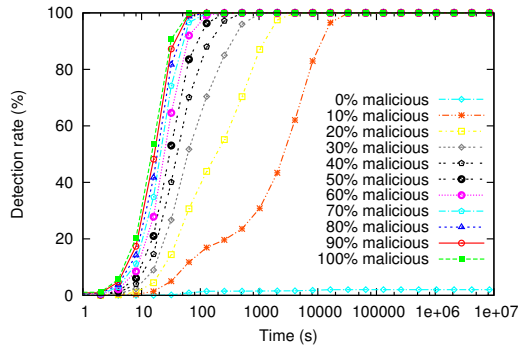


Fig. 9. Nodes detection percentage according to multiple malicious behavior, with α=1 and σ=1

tuning the aggressiveness of the detection, according to the requirements of the application.

VIII. Simulation Study

A. Analytical and Simulation Setup

We evaluate the performance of our model by focusing on its ability to detect and evict malicious nodes, and to incite selfish nodes to cooperate more. In our scenario, a malicious node is a node that creates and sends false information, and that corrupts data before sending it during a retransmission. Moreover, a malicious node can "cheat" and use a suitable signaling value for it. We assume, in

TABLE II
PARAMETER VALUES FOR THE SIMULATION

Number of nodes: 500	Mac layer protocol: IEEE 802.11p
Transmission range: 250m	Simulation time: 3600s, and 10800s
Urban area size: $6 \times 6\ Km^2$	Highway length: 35 Km
Urban speed: 20-50 km/h	Highway speed: 90-160 km/h
Arrival intensity λ=1 and 0.2	Diffusion data algorithm: ADCD [2]
C_{msg}=$C(Y^{\star}, \theta_{initial})/\mu$	Data rate: 6 Mbps
β=5	α=2.3
σ=5	$\theta_{initial}$=100
ρ=0.5	γ=20%
η=10%	μ=5

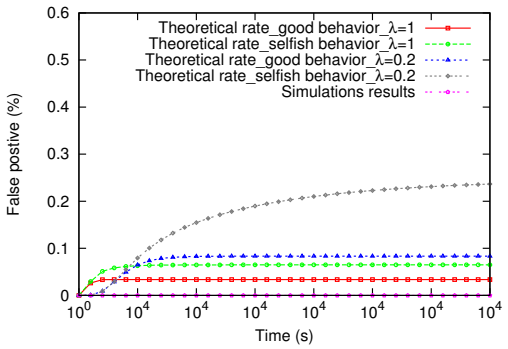


Fig. 11. Percentage of false positive

both theoretical and simulations analysis, that in order to mislead other nodes, a malicious node uses a signal value of $Y^{\star}(\theta_{initial})$ when its credits is lower than $\theta_{initial}$. On the other hand, selfish nodes only participate out of self-interest (i.e. when they do not have enough credit to decrypt received messages), we suppose that this threshold is fixed to $\theta_{initial}$ value. To this end, we first measure the detection rate with both theoretical and simulation analysis. Next, we study the average ratio of corrupted data, in a network composed of 16% and 25% of malicious nodes. Finally, the average data reception ratio is measured in a network composed of 25% and 50% of selfish nodes. Furthermore, for each analysis we set the arrival intensity parameter of detected events λ to 1 event per second, for a deployed VANET application in an average sized area, sharing events such as dangerous road features, accidents and traffic improvements; and 1 event every 5 seconds, for applications with stricter requirements on generated overhead.

We compare our simulation results to theoretical results, obtained with MATLAB. For simplicity, our theoretical study does not include a reputation model. Therefore, for realism purposes, we assumed that a node's behavior is composed of two types of behavior. Consequently, in our study, a predominantly good behavior node has up to 80% good behavior and up to 20% malicious behavior. Thus, its reputation is 100%. Similarly, a predominantly malicious node is up to 80% malicious. Finally, a predominantly selfish node is up to 80% selfish and 20% malicious. To compute the detection rates for different times, we provide each node with an initial credit value of 100, we assume a range of $[0, 500]$ for its variations, and we vary the arrival intensity parameter, λ, which defines the frequency of events to share for the nodes. We set the probability of collision, P_c, to 0.02, and the stationary probability of connection between nodes, π, to 0.01.

The simulations are conducted using NS2-34 [34] using the 802.11p extension for the MAC layer, with two different mobility scenarios. The first is a highway mobility scenario, generated with VanetMobisim [35], in a stretch of highway of $35km$, with a velocity ranging between $90km/h$ and $160km/h$. The second scenario is an urban mobility scenario generated with SUMO [36], in an area of 36 km^2, with a velocity ranging between $20km/h$ and $50km/h$. Since VanetMobisim is very accurate for highway scenarios, and Sumo is more often used to generate urban topologies [37]. We simulated 500 nodes in a urban and highway areas during 3600s when the arrival intensity of events λ is 1, and during 10800s when λ is 0.2. We set the transmission range to 250m and data rate to 6 Mbps. The simulation parameters are shown in Table II.

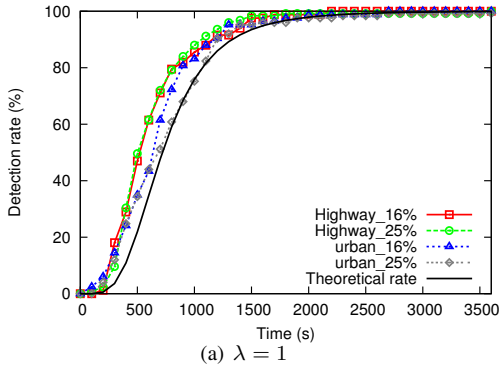
To study DTM^2's performance, we select three metrics for our evaluation:

- The detection malicious node delay and percentage of both malicious and no-malicious nodes (this later represents false positive percentage).
- The ratio of received and accepted false messages by the nodes at their detriment, in the presence of malicious nodes.
- The ratio of received data, in the presence of selfish nodes.

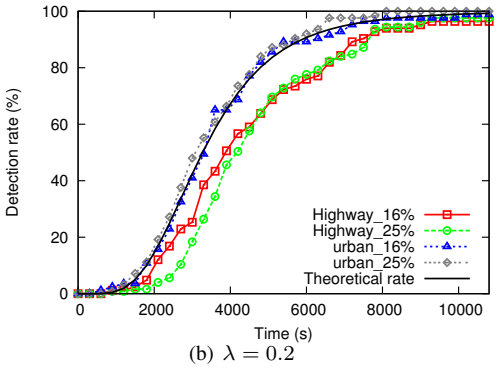
All the metrics have been studied for different compositions for the network according to the proportion of malicious and selfish nodes, with two values for the data arrival intensity frequency, in both urban and highway scenarios.

B. Detection Delays and Percentage

Fig. 10(a) and Fig. 10(b) present the malicious node detection rate for different times, which corresponds to malicious nodes running out of credit during 3600s and 10800s simulation times, respectively. In Fig. 10(a) one event is shared each second (λ =1), while in Fig. 10(b), one event is detected and shared every 5 seconds ($\lambda = 0.2$). In both figures, we compare the simulation results in highway and urban scenarios to the theoretical ones. We notice that the results are coherent. The detection rate reaches 50% between 500s and 700s. At 2000s the detection rate exceeds 98%, and 100% malicious node detection is achieved around 3000s. Compared to Fig. 10(a), the results of Fig. 10(b) reach 100% later in the simulation, this is due to the infrequent shared messages between nodes compared to the former case. Indeed, with less messages to send and less received messages, reputation values take more time to become meaningful. Likewise, the credit count of malicious nodes decreases slowly when they share less messages. This induces a detection rate of 50% reached by the urban scenarios after 3300s, and by highway scenarios at 4100s.

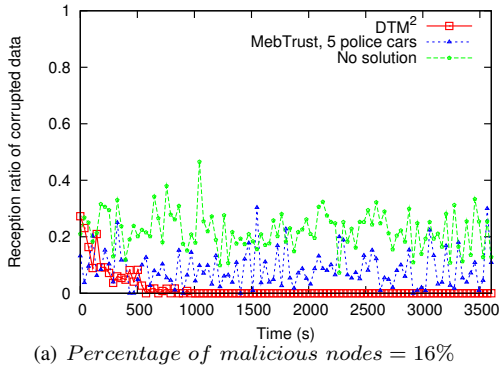


(a) $\lambda = 1$

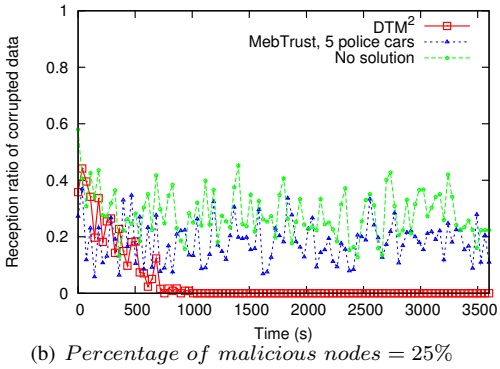


(b) $\lambda = 0.2$

Fig. 10. Percentage of detected malicious nodes



(a) *Percentage of malicious nodes* = 16%



(b) *Percentage of malicious nodes* = 25%

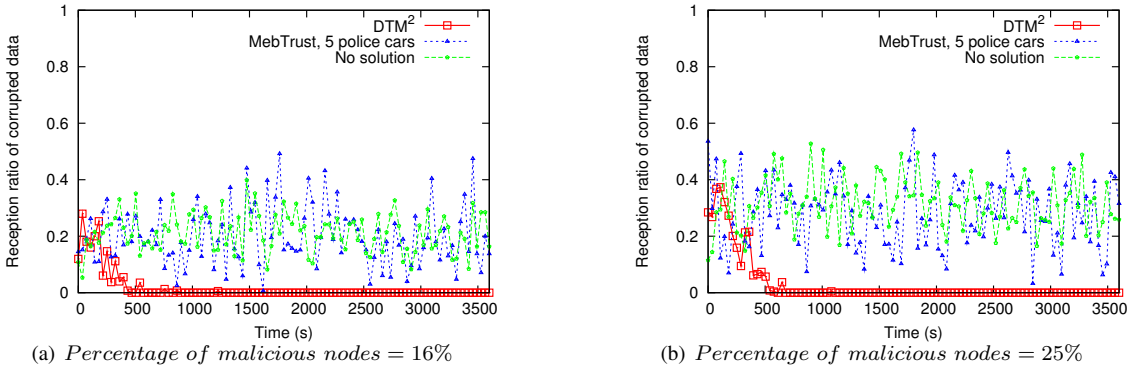
Fig. 12. Average received ratio of corrupted data in urban scenario, with $\lambda = 1$

For a detection rate of 75%, this occurs at 4400s and 5900s for urban and highway scenarios respectively. 96% is reached at around 7000s and 9000s. We notice that the factor of difference in times between the detection rates with λ =1 and λ =0.2 is in urban scenarios around 4.71, 4.88 and 4, 37 for 50%, 75% and 96%, respectively, and in highway scenarios around 8.2, 7.86 and 6, 42. This means that the detection time of all malicious nodes in a network is not automatically multiplied by the event frequency, but can be lower or greater because of the node distribution.

Besides the arrival intensity factor, which impacts the result, we observe from the two figures that the mobility patterns, and the network composition also have an impact, with different degrees. In fact, in Fig. 10(a), the shared messages are so frequent, that the nodes' reputations are quickly established, which leads to an effective decision for received messages in the network, for both acceptance or refusal. So, the remaining credits quickly diminish for malicious nodes, and they are rapidly excluded. Despite the superposition between the two highway scenarios curves, which means that the network composition does not have much impact in this case, there are no significant variations compared to the urban scenarios results, mostly from 1200s. The little variations can be caused by either the message loss because of the significant collision factor in urban scenarios, since the detection times are inversely proportional to the number of exchanged messages; or the difference in node connectivity in urban and highway scenarios, as in an urban scenario, a node's neighbors change more frequently than in an highway scenario, thus inducing positive and negative points. A drawback of frequent changes is that it takes a long time to establish valid reputation values, compared to a highway scenario, as resulted in Fig. 10(a). However, the advantage is that a node posses a larger global view of the reputation of the node in the network, we notice this in Fig. 10(b) and conversely to the first case, the results are better in urban scenarios than in the highway, independently of the network composition. The frequent neighborhood changes in urban scenario allows to retransmit received information more frequently, thus spending or earning more often credits, and holding larger view of the network. In contrast, highway scenarios have a lot of constant trajectories inducing limitations in data retransmission, accurate reputation about direct neighbors, and very often none about the others.

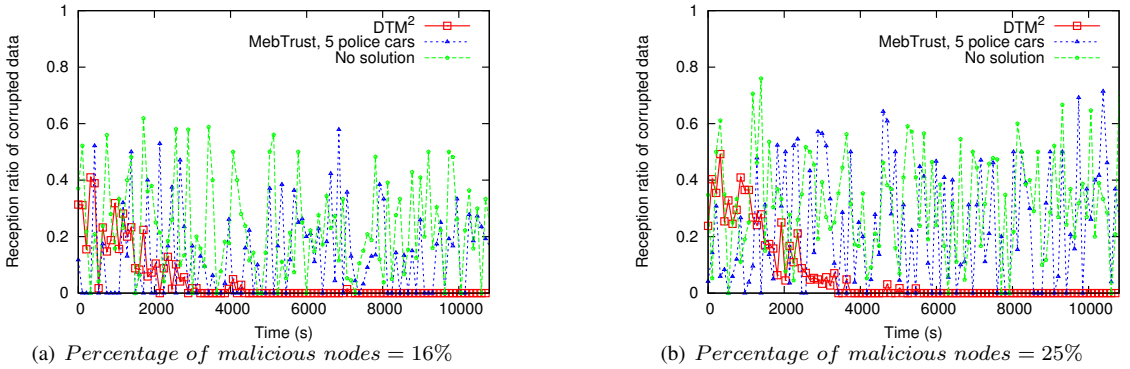
C. False Positive

False positive results are illustrated in Fig. 11, we collect and compare the detection percentage of the good and selfish nodes during more than 19 hours. For this study, we set the arrival intensity parameter λ to 1, then to 0.2, in both theoretical and simulation analysis. Since the



(a) $Percentage\ of\ malicious\ nodes = 16\%$ (b) $Percentage\ of\ malicious\ nodes = 25\%$

Fig. 13. Average received ratio of corrupted data in highway scenario, with $\lambda = 1$



(a) $Percentage\ of\ malicious\ nodes = 16\%$ (b) $Percentage\ of\ malicious\ nodes = 25\%$

Fig. 14. Average received ratio of corrupted data in urban scenario, with $\lambda = 0.2$

simulation results in all the scenarios are identical and equal to zero, we represent them in only one curve. The remaining curves ensure the stability of the very low risk of having a false positive detection, by reaching stationary probabilities, which means that whatever the simulation duration, never the probability of detecting will exceed a certain probability. The stationary probability for detecting a good behavior node is equal to 0.0336701% and reached after 8300s when $\lambda = 1$, and is equal to 0.0833375% reached after 42500s when $\lambda = 0.2$. The stationary probability for detecting a selfish node is equal to 0.0648695% after 43100s when $\lambda = 1$. In the case where $\lambda = 0.2$, the probability increases because of the low number of message to share, thus, less opportunity for a selfish node to raise its credits. However the probability remains very low, equal to 0.236583% at 70000s. The low false positive percentage is obtained mainly because of the assumption of credit safeguard, where a node does not accept received messages when its credit level is too low ($\theta \leq \theta_{initial} \times \eta$). During our simulation we chose $\eta = 10\%$.

This three figures show the stability of the obtained results, that a detection of 100% is always reached after a certain time, and particularly that the false positive rate is lower than 0.5% and does not increase later.

D. False Message Diffusion

A direct consequence of the presence of malicious nodes in a network, is the sharing of false and tampered data, or its unknowing retransmission by good behavior nodes. To study this harmful impact, we gather the ratio of false messages that nodes receive and accept (i.e. considering them as valid) in several times, and in different network conditions.

We compare DTM^2's results with those of a network without any solution, and with a network using a majority-based and experience-based trust model presented in [19], which we refer to as MEB_Trust.

The basic idea in MEB_Trust is that a node asks its neighbors about the truthfulness of a received data. After receiving more than the minimum number of responses fixed by the application, the vehicle computes the majority opinion of the received responses. The vehicle gives more weight to the responses sent by vehicles that have higher categories, such as police vehicles in MEB_Trust case, and those who have larger experience-based trust values. According to the majority opinion, they accept or not the received data.

Authors in [19] study the performance of their proposed solution by observing the traffic congestion caused by the dissemination of untruthful velocity information. Indeed, malicious nodes in [19] send false velocity information to cause traffic congestion. Authors measure the average road speed. The lower the speed is, the higher the impact of

untruthful data.

We choose to compare DTM^2 with this solution for the metric of average received corrupted data ratio. Our solution, DTM^2 does not detect only false velocity information, but all corrupted traffic information. As DTM^2, MEB_Trust helps a node to validate or remove a received message. However, this solution depends on the presence of trusted entities (e.g. police cars), which always respond correctly to nodes, but does not exclude malicious nodes. For our simulation of this solution we included 5 police cars (1%), which is an average value with respect to those used in the original paper [19].

Fig. 12 and Fig. 13 present the average received ratio of false data in both urban and highway scenarios respectively, with $\lambda = 1$. We performed a series of tests by modifying the percentage of malicious nodes in the network from 5% to 50%. However, for clarity purposes, we chose to only present two scenarii (16% and 25%) as they clearly illustrate the evolution of the detection process.

In both Figs. 12(a) and 12(b), we note that when using DTM^2, the ratio of false received data quickly decreases until reaching 0 after 1000s of simulated time for a network composed of 16% and 25% in an urban scenario. We notice that this time is lower than the one to detect and evict 100% malicious nodes in the same conditions. This means that nodes come up to successfully decide to accept or to refuse a received message thanks to the use of reputations and signal values, well before malicious nodes deplete their credits, which means that some nodes are able to recognize some malicious nodes before their exclusion. Concerning the two other solutions, the results of Meb_Trust are better than those without solution, which never reach to zero, as it is the case for DTM^2. In addition, Meb_Trust efficiency is not scalable, since when more than 16% malicious nodes are present, the results deteriorate. Moreover, DTM^2 is able to better control oscillations in Fig. 12(a) and Fig. 12(b), compared to the two other solutions.

The results in both Fig. 13(a) and Fig. 13(b) are similar to those in an urban scenario. Therefore, we conclude that while the arrival intensity is high, the mobility scenario has less impact on the detection percentage since the large number of exchanged messages with $\lambda = 1$ fades of the network differences between urban and highway scenarios, because of collisions and frequent neighborhood changes. DTM^2 in a highway scenario, with $\lambda = 1$, efficiently and rapidly copes with the presence of malicious nodes.

When events to share are scarce, as in Fig. 14, reception ratio of false data changes more for the three deployed solutions, and its maximum values are higher than with $\lambda = 1$. This is due to a lower knowledge of nodes about their surrounding. The reputation values are less accurate, which induces good behavior nodes to accept and share false date longer. In Fig. 14(a), the average received ratio of corrupted data in DTM^2 reaches zero after 4400s simulation time, and after 5500s in Fig. 14(b). We notice that the network with Meb_Trust and with no solution also have difficulties to limit ratio of false received data. In the case of Meb_Trust, the solution is essentially based on trust vehicle presence as police car, and on reputation values, these values have difficulties to converge with the presence of numerous malicious node. Even if the ratio with Meb_Trust reaches zero often, this occurs when an event is detected and forwarded by good behavior nodes, or when shared false data is removed by trusted vehicles. However, large oscillations remain because of the infrequent meetings with trust vehicles, which makes the solution inefficient to cope with malicious nodes in highly mobile and large networks as VANET.

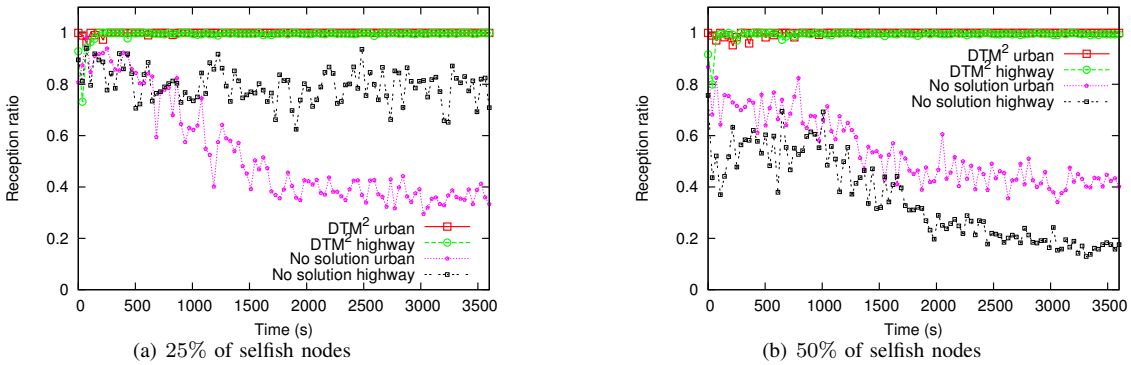
E. Network Cooperation in the Presence of Selfish Nodes

The last metric to study, in order to validate DTM^2, is the nodes' cooperation. Therefore, we calculate the ratio of received truthful data by the concerned nodes about each event. This ratio is directly impacted by the presence of selfish nodes, which refuse to cooperate. We suppose that selfish nodes are rational, so they cooperate only when they need credits to their own interest, as receiving other messages, we fix the threshold of selfish node cooperation to the credit initial value, $\theta_{initial}$. We compute this ratio in several network conditions, in a network using DTM^2 and without any solution.

Fig. 15(a) and Fig. 15(b) present the reception ratio of data for concerned nodes in urban and highway scenarios when $\lambda = 1$, for 25% and 50% selfish nodes in the network respectively. Ratios in urban and highway with DTM^2 perfectly overlap, and are equal to 1 from the simulation start, since selfish nodes need credits to pay for their numerous received messages. We noticed that in the case with no deployed solution, the impact of selfish nodes is huge, even in a network with only 25% selfish nodes. Since they have no incentive to cooperate, and no constraint if they refuse, selfish nodes do not cooperate. Their impact on the urban scenario without deployed solution is high enough, but invariant with their percentage. Unlike in a highway scenario, where the ratio is less affected with 25% selfish node presence than with 50%, this can be caused by the nodes' constant trajectories in such a scenario. Indeed, if a node has 50% selfish neighbors over a long period, and follows a constant trajectory, it and its neighbors can often share the same neighbors, which reduces the detected and retransmitted events. So, a node receives fewer messages with 50% of cooperative and constant neighbors than if it has 50% of cooperative and mobile ones. In an urban scenario, the 50% of cooperative neighbors have a higher chance of receiving and retransmitting a lot of messages, thanks to their different surroundings.

IX. Conclusion

In this paper, we proposed DTM^2, a Distributed Trust Model for VANETs, adapted from the job market signaling model, a well-known economic model used in the case where asymmetric information is held between parties. DTM^2



(a) 25% of selfish nodes (b) 50% of selfish nodes

Fig. 15. Average received ratio, with selfish node presence, and $\lambda = 1$

focuses on managing a tamper-proof credit count received by nodes at the start of the application. In order to detect and evict malicious nodes, it creates self-selection among the network's nodes and exhausts the credit for those nodes with bad behavior. Moreover, to improve the cooperation level of selfish nodes, it proposes inciting rewards. In order to tune the different parameters involved in DTM^2 behavior, we model it using a Markov chain. Then, we showed via simulation the achievement of the two DTM^2 objectives (i.e. evicting malicious nodes and encouraging selfish ones to cooperate) in networks composed of 25%, or 50% of malicious or selfish nodes. In both of these cases, DTM^2 is able to gradually detect *all* malicious nodes and completely eliminate their negative effects on the network, while avoiding the erroneous detection of good or selfish behavior nodes. Furthermore, our approach is able to increase the cooperation of selfish nodes by maintaining a high reception ratio, unlike networks where no solution is offered.

REFERENCES

[1] Y. Toor, P. Muhlethaler, and A. Laouiti, "Vehicle ad hoc networks: applications and related technical issues," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 3, pp. 74–88, 2008.

[2] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane, "Modeling and performance evaluation of advanced diffusion with classified data in vehicular sensor networks," *Wireless Communications and Mobile Computing*, vol. 11, no. 12, pp. 1689–1701, Oct. 2011.

[3] C. Wu, S. Ohzahata, and T. Kato, "A broadcast path diversity mechanism for delay sensitive vanet safety applications," in *IEEE VNC*, Amsterdam, The Netherlands, 2011.

[4] M.Spence, "Job market signaling," *The Quarterly Journal of Economics*, vol. 87, no. 3, pp. 355–374, 1973.

[5] J. Sobel, "Signaling games," *Computational Complexity Theory, Techniques, and Applications*, pp. 2830–2844, 2012.

[6] M.Spence, "Signaling in retrospect and the informational structure of markets," *The American Economic Review*, vol. 92, no. 3, pp. 434–459, 2002.

[7] E. Baccelli, P. Jacquet, B. Mans, , and G. Rodolakis, "Information propagation speed in bidirectional vehicular delay tolerant networks," in *IEEE INFOCOM*, Shanghai, China, April 2011.

[8] N. Haddadou and A. Rachedi, "Dtm^2: Adapting job market signaling for distributed trust management in vehicular ad hoc networks," in *IEEE ICC*, Budapest, Hungary, June 2013.

[9] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile ad hoc networks: A survey," *IEEE Communications Surveys and Tutorials*, vol. Preprint, pp. 1–20, 2011.

[10] L. Buttyán and J. Hubaux, "Enforcing service availability in mobile ad-hoc wans," in *ACM MobiHoc*, Boston, USA, Aug 2000.

[11] ——, "Stimulating cooperation in self-organizing mobile ad hoc networks," *ACM/Kluwer MONET*, vol. 8, pp. 579–592, 2001.

[12] Z. Zhang, G. Mao, and B. D. O. Anderson, "On the information propagation process in multi-lane vehicular ad-hoc networks," in *IEEE ICC*, Ottawa, Canada, June 2012.

[13] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane, "Trust and exclusion in vehicular ad hoc networks: an economic incentive model based approach," in *ComComAp*, Hong Kong, China, April 2013.

[14] A. Rachedi, A. Benslimane, H. Otrok, N. Mohammed, and M. Debbabi, "A secure mechanism design-based and game theoretical model for manets," *Mobile Networks and Applications*, vol. 15, no. 2, pp. 191–207, 2010.

[15] F. Li and J. Wu, "Frame: an innovative incentive scheme in vehicular networks," in *IEEE ICC*, Dresden, Germany, June 2009.

[16] F. Tseng, Y. Liu, J. Hwu, and R. Chen, "A secure reed-solomon code incentive scheme for commercial ad dissemination over vanets," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 9, pp. 4673–4731, Nov. 2011.

[17] S. Zhong, J. Chen, and Y. Yang, "Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks," in *IEEE INFOCOM*, San Francisco, USA, Apr. 2003.

[18] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," *Journal of the Society for Industrial and Applied Mathematics*, vol. 8, no. 2, pp. 300–304, 1960.

[19] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "A multifaceted approach to modeling agent trust for effective communication in the application of mobile ad hoc vehicular networks," *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, vol. 41, no. 3, pp. 407–420, May 2011.

[20] M. Ashtiani and Q. Dongyu, "Achieving fair cooperation for multi-hop ad hoc networks," in *QBSC*, Queen's University Kingston, Canada, May 2010.

[21] A. Rachedi and A. Benslimane, "Toward a cross-layer monitoring process for mobile ad hoc networks," *Security and Communication Networks, John Wiley InterScience*, vol. 2, no. 4, pp. 351–368, 2009.

[22] The Trusted Platform Module (TPM) website. [Online]. Available: https://www.trustedcomputinggroup.org/groups/tpm/

[23] G. Guette and O. Heen, "A tpm-based architecture for improved security and anonymity in vehicular ad hoc networks," in *VNC*, Tokyo, Japan, Oct. 2009.

[24] G. Guette and C. Brce, "Using tpms to secure vehicular ad-hoc networks (vanets)," in *WISTP*, Sevilla, Spain, May 2008.

[25] J. Wanga, Y. Liu, and Y. Jiao, "Building a trusted route in a mobile ad hoc network considering communication reliability and path length," *Journal of Network and Computer Applications*, vol. 34, no. 4, pp. 1138–1149, 2011.

[26] X. Zhang, M. Zhou, J. Zhuang, and J. Li, "A multi-channel vanet providing concurrent safety and commercial services," in *VANET '05*, New York, NY, USA, 2005.

[27] T. K. Mak, K. P. Laberteaux, and R. Sengupta, "Implementation of ecc-based trusted platform module," in *International Conference on Machine Learning and Cybernetics*, Hong Kong, 2007.

[28] N. Kuntze and A. Schmidt, "Trusted ticket systems and applications,"

Trusted Computing - Challenges and Applications. Lecture Notes in Computer Science, vol. 232, pp. 49–60, 2007.
[29] M.Spence, *Market Signaling: Informational Transfer in Hiring and Related Screening Processes*. Harvard economic studies, 1974.
[30] Z. Charikleia, L. Brian, H. Marek, and K. Roshan, "Robust cooperative trust establishment for manets," in *ACM SASN*, New York, USA, 2006.
[31] S. Ni, Y. Tseng, Y. Chen, and J. Sheu, "The broadcast storm problem in a mobile ad hoc network," in *MobiCom*, Washington, USA, August 1999.
[32] M.I.Hassan, H. Vu, and T.Sakurai, "Performance analysis of the ieee 802.11 mac protocol for dsrc safety applications," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 8, pp. 3882–3896, 2011.
[33] J. Whitbeck, V. Conan, and M. D. de Amorim, "Performance of opportunistic epidemic routing on edge-markovian dynamic graphs," *IEEE Transactions on Communications*, vol. 59, no. 5, pp. 1259–1263, May 2011.
[34] The NS-2 website. [Online]. Available: http://www.isi.edu/nsnam/ns/
[35] M. Fiore, J. Härri, F. Fethi, and C. Bonnet, "Vehicular mobility simulation for vanets," in *IEEE ANSS*, Norfolk, USA, Mar. 2007.
[36] Sumo project. [Online]. Available: http://sourceforge.net/projects/sumo//
[37] S. Busanelli, G. Ferrari, and V. A. Giorgio, "I2v highway and urban vehicular networks: A comparative analysis of the impact of mobility on broadcast data dissemination," *Journal of Communications*, vol. 6, no. 1, pp. 87–100, 2011.

Nadia Haddadou received the M.Sc. degree in Computer Science from UPMC Sorbonne Universités in Paris, France, in 2010. She obtained her Ph.D. in computer networks from University Paris-Est Marne-la-Vallée, in 2014. Her research interests are vehicular networks and security. She was assistant professor (ATER) at the university Paris-Est Marne-la-Vallée (UPEM) in 2014.

Abderrezak Rachedi received his engineer degree in computer science from the university of technology and science (USTHB), Algiers, Algeria, in 2002 and research MS and professional MS degrees in computer science from the University of Savoie and University of Lyon in France in 2003 and 2005, respectively. He received his Ph.D. degree in computer science from the university of Avignon, France, in 2008.

He was assistant professor (ATER) at the university Paris-Est Marne-la-Vallée (UPEM) in 2008. He is currently working as associate professor (maître de conférences) at the university Paris-Est Marne-la-Vallée (UPEM) and a member of the Gaspard Monge Computer Science Laboratory (LIGM CNRS UMR 8049) since September 2009.

His research interests lie in the field of wireless networking, wireless multi-hop networks, wireless sensor networks, vehicular networks, performance evaluation, quality of services and security. He is an author or co-author of over 60 papers in technical journals and international conferences. He participated or still participates to several national and international research projects. Among them ANR CLADIS (2006-2009), Digiteo ViSuNet (2010-2013), RECASURG-UTIC (2011-2013), PPS-WSNTM (2011-2014), MMASP-COFECUB (2012-2015), CarCode-ITEA3 (2012-2015).

Dr Rachedi serves as Associate Editor of Wireless Communications and Mobile Computing (WCMC) journal and International Journal of Communication Systems (IJCS). He also served on the Editorial Boards of Journal of Computer Systems, Networks, and Communications (JCSNC). He has been on the technical program committee of different ACM and IEEE conferences, including Globecom, ICC, WiMob, WCNC, IWCMC and chaired some of their sessions. Dr Rachedi is an IEEE member.

Yacine Ghamri-Doudane is currently Full Professor at the University of La Rochelle (ULR) in France, and member of its Laboratory of Informatics, Image and Interaction (L3i). Before that, Yacine held an Assistant/Associate Professor position at the ENSIIE, a major French post-graduate school located in Evry, France, and was a member of the Gaspard-Monge Computer Science Laboratory (LIGM - UMR 8049) at Marne-la-VallÃ©e, France. From February 2011 till July 2012, he was regularly visiting the Performance Engineering Laboratory of University College Dublin, Dublin, Ireland. Yacine received an engineering degree in computer science from the National Institute of Computer Science (INI), Algiers, Algeria, in 1998, an M.S. degree in signal, image and speech processing from the National Institute of Applied Sciences (INSA), Lyon, France, in 1999, a Ph.D. degree in computer networks from University Pierre and Marie Curie, Paris 6, France, in 2003, and a Habilitation to Direct Research (HDR) in Computer Science from UniversitÃ© Paris-Est, in 2010.

His current research interests lays in the area of wireless networking and mobile computing with a current emphasis on topics related to the Internet of Things (IoT), Wireless Sensor Networks (WSN) and Vehicular Networks. Yacine holds three (3) international patents and he authored or co-authored seven (7) book chapters, twenty (20) peer-reviewed international journal articles and more than 70 peer-reviewed conference papers. Since 1999, he participated or still participates to several national and European-wide research projects in its area of interests. Among them two regional research projects, two national-wide research projects, nine European-wide research projects (five on-going ones in 2014-2015) as well as two EU COST Actions. As part of his professional activities linked to the computer networking research community, Yacine also acted as the Chair the IEEE Communications Society (ComSoc) Technical Committee on Information Infrastructure Networking (TCIIN - previously TCII) from January 2010 till December 2013 and he is currently chairing the IEEE ComSoc Humanitarian Communications Technologies Ad hoc Committee (HCTC). He is an editorial board member of Elsevier ComNet, Elsevier JNCA and Wiley WCMC Journals as well as the founding co-editor of the IEEE ComSoc Ad Hoc and Sensor Network Technical Committee (AHSN TC) Newsletter. Among other conference involvements, he is currently acting as the TPC Chair of IEEE CCNC 2015 and acted or still act as Symposium co-Chair in IEEE ICC 2009, 2010 and 2012 as well as IEEE GLOBECOM 2012 and 2015. He is a Member of IEEE.